ESTADISTICA

MINISTERIO DE SALUD
INSTITUTO DE GESTIÓN DE SERVICIOS DE SALUD
HOSPITAL "SERGIO E. BERNALES"

Nº 033 – 2015 – DG-HSEB.

RESOLUCIÓN DIRECTORAL

Comas, 27 ENE. 2015

Visto el Memorando N° 297-2014-OEI-HNSEB, emitido por la Oficina de Estadística e Informática, que solicita la revisión y aprobación de la "Directiva de Seguridad de la Información para el Acceso a la Información, Servicios y Equipos Informáticos en el Hospital Sergio E. Bernales", y;

CONSIDERANDO:

Que, la Ley N° 28716, Ley de Control Interno de las Entidades del Estado, establece entre otros aspectos el Sistema de Control Interno, indicando que su implementación y funcionamiento está a cargo de las autoridades y funcionarios de cada entidad pública;

Que, mediante Resolución Ministerial N° 1942-2002-SNDM se aprobó la Directiva N° 001-2002-OGEI "Normas Generales sobre acciones del sistema de Información, Estadística e Informática del ministerio de Salud;

Que, mediante Resolución Ministerial N° 520-2006/MINSA, se aprueba el documento técnico "Lineamientos de Política de Seguridad de la Información del Ministerio de Salud";

Que, mediante Resolución Ministerial N° 971-2006/MINSA, se aprueba la Directiva Administrativa N° 100-MINSA/OGEI-V.01 "Directiva Administrativa para el correcto uso de equipos de cómputo y servicios informáticos del Ministerio de Salud".

Que, mediante Resolución de Contraloría N° 072-98-CG, se emiten las Normas de Control Interno para el Sector Publico, en la cual se indica la NCI 500 – Normas de Control Interno para sistemas Computarizados;

Que, en ese contexto, la Oficina de Estadística e Informática ha elaborado el proyecto de Directiva Administrativa denominado "Directiva de Seguridad de la Información para el Acceso a Información, Servicios y Equipos Informáticos en el Hospital Sergio E. Bernales" y que mediante Memorando N° 297-2014-OEI-HNSEB lo deriva a la Oficina Ejecutiva de Planeamiento Estratégico para su revisión;

Que mediante Informe N° 003-2015-OEPE-HSEB, el Director Ejecutivo de la Oficina Ejecutiva de Planeamiento Estratégico deriva el Informe N° 002-2015-EQ.ORGANIZACION-OEPE-HSEB elaborado por el Equipo de Trabajo de Organización, en el cual se indica que luego de la revisión del proyecto de documento técnico y coordinación con la Oficina de Estadística e Informática para su corrección correspondiente se emite opinión técnica favorable y por tanto propone su aprobación vía acto resolutivo;

Que, la Directiva propuesta por la Oficina de Estadística e Informática, tiene como objetivo establecer las responsabilidades, principios, criterios, directrices y conductas dentro de los lineamientos de ética y el buen gobierno electrónico para los servicios en el Hospital Sergio E. Bernales;

Que, dentro de este contexto, es necesario formalizar un Documento Técnico que tenga la finalidad de dar a conocer las políticas y estándares de seguridad informática que deben tomar en cuenta los usuarios de los servicios informáticos y tecnologías de información, para proteger adecuadamente los activos tecnológicos y la información que se maneja en el Hospital Sergio E. Bernales;

Con las visaciones del Director Adjunto, Director Ejecutivo de la Oficina Ejecutiva de Planeamiento Estratégico y del Jefe de la Oficina de Asesoría Jurídica del Hospital "Sergio E. Bernales" ;

De conformidad y en uso de las atribuciones conferidas en el artículo 11ª del Reglamento de Organización y Funciones del Hospital "Sergio E. Bernales", aprobado mediante Resolución Ministerial N° 795-2003-SA/DM y modificado mediante Resolución Ministerial N°512-2004-MINSA, Resolución Ministerial N°343-2007-MINSA y Resolución Ministerial N°124-2008-MINSA;

SE RESUELVE:

Artículo 1°. - Aprobar, la directiva Administrativa N° 001-2015-HSEB/OEI "Directiva de Seguridad de la Información para el Acceso a la Información, Servicios y Equipos Informáticos en el Hospital Sergio E. Bernales" el mismo que en documento anexo forma parte integrante de la presente Resolución.

Artículo 2°.- Encargar, a la Oficina de Estadística e Informática la difusión, supervisión e información del cumplimiento de la Directiva aprobada en el artículo precedente.

Artículo 3°.- Dejar sin efecto cualquier acto resolutivo o acto de administración precedente que se oponga a la presente Resolución.

Artículo 4°.- Disponer que la Oficina de Comunicaciones publique la presente Resolución Directoral y el correspondiente Documento Técnico, en el Portal de Internet del Hospital "Sergio E. Bernales"

Regístrese, Comuníquese

JAAT/mse

MINISTERIO DE SALUD
Hospital Nacional Sergio E. Bernales
Jaime A. Arévalo Torres
DIRECTOR GENERAL
CMP. Nº 25856

Asesoría Jurídica - Hospital Sergio E. Bernales
V°B°

HOSPITAL NACIONAL SERGIO E. BERNALES
OFICINA DE ESTADÍSTICA E INFORMÁTICA

DIRECTIVA ADMINISTRATIVA N° 001-2015-HSEB/OEI

DIRECTIVA DE SEGURIDAD DE LA INFORMACION PARA EL ACCESO A INFORMACION, SERVICIOS Y EQUIPOS INFORMATICOS EN EL HOSPITAL SERGIO E BERNALES

I. FINALIDAD

Dar a conocer las políticas y estándares de Seguridad informática que deben tomar en cuenta los usuarios de los servicios de tecnologías de información, para proteger adecuadamente los activos tecnológicos y la información que se maneja en el Hospital Sergio E. Bernales.

II. OBJETIVO:

2.1. OBJETIVO GENERAL

Establecer las responsabilidades, principios, criterios, directrices y conductas dentro de los lineamientos de ética y el buen gobierno electrónico para los servicios hospitalarios y/o oficinas del Hospital Sergio E. Bernales.

2.2. OBJETIVO ESPECIFICO

- Establecer las Políticas y Estándares de Seguridad Informática a todo usuario que interactúa con equipos y/o servicios informáticos Hospital Sergio E. Bernales.
- Orientar al usuario informático sobre el correcto usó y cuidado de su equipo informático.
- Definir procedimiento para adquirir servicios informáticos en el Hospital Sergio E. Bernales.

III. AMBITO DE ABLICACION

La presente directiva es de aplicación permanente y de cumplimiento obligatorio para todos los órganos de línea, de asesoramiento y apoyo, alcanzando también a contratistas que interactúan con equipos y/o servicios informáticos del Hospital Sergio E. Bernales.

IV. BASE LEGAL

- LEY N° 27657 – LEY DEL MINISTERIO DE SALUD

- R.M. N° 795-2003/SA/DM-Aprueba el Reglamento de Organización y funciones del Hospital Sergio E. Bernales, modificado por la RD N° 512-2004-MINSA
- R.M. N° 520-2006/MINSA, que aprueba el Documento Técnico "Lineamientos de Política de Seguridad de la Información del Ministerio de Salud"
- Directiva Administrativa N° 100-MINSA7OGEI-V0. 1 "Directiva Administrativa para el correcto uso de Equipos de cómputo y Servicios Informáticos del Ministerio de Salud".
- Directiva N°008-95-INEI/SJI "Recomendaciones Técnicas para la Protección Física de los equipos y medios de Procesamiento de la información en la Administración Publica.
- Directiva N° 007-95-INEI/SJI "recomendaciones Técnicas para la seguridad e integridad de la información que se procesa en la administración pública.
- Directiva Administrativa N° 087-MINSA/OGEI-V0.1: "Directiva Administrativa para el correcto uso de Equipos de Cómputo y Servicios Informáticos del Ministerio de Salud".
- Resolución de Contraloría N° 072-98 CG- Normas de control Interno para el Sector Publico: 500-Normas de control Interno para Sistemas Computarizados.
- Manual de Organización de Funciones para el área de estadística.
- R.M. N° 526-2011/MINSA "Normas para la Elaboración de Documentos Normativos del Ministerio de Salud"

V. DISPOSICIONES GENERALES

5.1. DEFINICIONES OPERATIVAS

1. **Administrador del sistema.** Persona responsable de administrar, controlar, supervisar y garantizar la operatividad y funcionalidad de los sistemas. Dicha administración está en cabeza de la Gerencia de informática.

2. **Administrador de correo.** Persona responsable de solucionar problemas en el correo electrónico, responder preguntas a los usuarios y otros asuntos en un servidor.

3. **Acceso Remoto:** Acceso a una estación de trabajo desde otro punto de acceso o de cualquier ordenador a través de Internet o la red.

4. **Antivirus:** Programa especializado en la detección y en la destrucción de virus informáticos.

5. **Autorización:** Función que permite otorgar acceso de uso de determinados recursos a un usuario dado.

6. **Archivo:** Sinónimo de fichero y esencia del almacenamiento informático.

7. **Backup:** Es la copia de seguridad de la información (total o parcial) del disco duro, de un CD u otro medio de almacenamiento informático

8. **Buzón:** También conocido como cuenta de correo, es un receptáculo exclusivo, asignado en el servidor de correo, para almacenar los mensajes y archivos adjuntos enviados por otros usuarios internos o externos a la empresa.

9. **Chat:** (Tertulia, conversación, charla). Comunicación simultánea entre dos o más personas a través de Internet.

10. **Computador:** Es un dispositivo de computación de sobremesa o portátil, que utiliza un microprocesador como su unidad central de procesamiento o CPU.

11. **Contraseña o password:** Conjunto de números, letras y caracteres, utilizados para reservar el acceso a los usuarios que disponen de esta contraseña.

12. **Correo electrónico:** También conocido como E-mail, abreviación de electronic mail. Consiste en el envío de textos, imágenes, videos, audio, programas, etc., de un usuario a otro por medio de una red. El correo electrónico también puede ser enviado automáticamente a varias direcciones.

13. **Cuentas de correo:** Son espacios de almacenamiento en un servidor de correo, para guardar información de correo electrónico. Las cuentas de correo se componen de un texto parecido a este mperez@hnseb.gob.pe donde

"mperez" es nombre o sigla identificadora de usuario, "hnseb " el nombre de la institución con la que se crea la cuenta o el dominio y ".gob.pe" una extensión propia de Internet según el dominio.

14. **Discos Flexibles:** Se usan como medio de almacenamiento secundario en microcomputadoras, cuyo uso ha sido generalizado por su facilidad de manejo y bajo costo.

15. **Disco Duro:** Es el dispositivo encargado de almacenar información de forma persistente en su ordenador.

16. **Equipos informáticos y comunicación:** Servidores de Red, estaciones de trabajo, impresoras y equipos de comunicaciones (swiches, hub, routers, etc.).

17. **Formatear:** Borrar por completo la información existente en un dispositivo de almacenamiento.

18. **Hardware:** se denomina así al conjunto de componentes físicos dentro de la informática (un teclado, una placa, por ej.).

19. **Identificador de Usuario de Pc:** Nombre con el que se ingresa al equipo asignado.

20. **Usuario de Sistema:** Nombre con el que se ingresa a algún sistema hospitalario o financiero dentro del HSEB.

21. **Páginas Web**: Forma de denominar a las hojas creadas con HTML que se manejan dentro del entorno WWW.

22. **Palabra Clave:** Palabra o código utilizado para identificar a un usuario autorizado; es normalmente provisto por el sistema operativo o por un sistema de Gestión de Base de Datos (SGBD), la computadora solo puede verificar la legitimidad de la contraseña y no la legitimidad del usuario.

23. **Programa:** Instrucciones que varían según el lenguaje que se utiliza, pero cuyo fin es el de controlar las acciones que tiene que llevar a cabo el ordenador y sus periféricos.

24. **Protección:** Mecanismo de control contra posibles acciones no autorizadas que brinda el sistema informático.

25. **Respaldo:** Se refiere a una copia extra, de un archivo o base de datos.

26. **Seguridad:** Medidas de resguardo contra el acceso no autorizado a los datos. Los programas y datos se pueden asegurar entregando números de identificación y contraseñas a los usuarios autorizados de una computadora.

27. **Servicio Informático:** Conjunto de actividades (planeamiento, análisis, diseño, programación, operación, entrada de datos, autoedición, bases de datos, etc.) asociados al manejo automatizado de la información que satisfacen las necesidades de los usuarios de este recurso.

28. **Software:** Todos los componentes informáticos de carácter no físico, sino lógico. Como pueden ser sistemas operativos, programas dedicados a la gestión de diseño, etc.

29. **USB:** (Universal Serial Bus) Unidad extraíble de almacenamiento

30. **Usuario:** Para efectos de las presentes normas, se entiende como usuario al funcionario, servidor o contratado bajo cualquier modalidad, que se encuentre en posesión de los bienes asignados (equipo de cómputo).

31. **Virus Informático:** Son programas creados por especialistas de computación con la finalidad premeditada de alterar el funcionamiento normal del computador. Un virus puede reproducirse, auto ejecutarse, ocultarse, infectar

otros tipos de archivos, encriptarse, cambiar de forma, residir en memoria, etc.

32. **OEI:** Oficina de Estadística e informática.

33. **HSEB:** Hospital Sergio E. Bernales

VI. DISPOSICIONES ESPECIFICAS.-

La presente considera los siguientes puntos:

- CONSIDERACIONES DE TODO USUARIO
- DE LA SEGURIDAD DE LA INFORMACION
- DE LA SEGURIDAD FISICA
- DEL MANEJO DE LA INFORMACION
- SOBRE EL SOFTWARE ADICIONAL
- SOBRE EL SOFTWARE DE ACCESO REMOTO
- SE LA SEGURIDAD DE LA RED
- DEL USO DEL CORREO INSTITUCIONAL
- DE LA SEGURIDAD CONTRA CODIGO MALISIOSO Y/O VIRUS
- SOBRE ACCESO DE INTERNET
- DE LOS CONTROLES DE ACCESO LOGICO
- RESPONSABILIDADES DE LOS USUARIOS
- DE LAS ACCIONES DE LA OEI
- DE LOS DERECHOS DE PROPIEDAD INTELECTUAL

CONSIDERACIONES DE TODO USUARIO

Artículo 1°.- Todo usuario de recursos, bienes y servicios informáticos debe conducirse bajo los principios de confidencialidad de la información y de uso adecuado de los recursos informáticos del Hospital Sergio E. Bernales.

Artículo 2°.- Es responsabilidad de los usuarios de bienes y servicios informáticos cumplir las Políticas y Estándares de Seguridad Informática.

Artículo 3°.- Todo empleado del de nuevo ingreso deberá: Leer presente directiva de Seguridad de la Información para Usuarios del HSEB.

Artículo 4°.- Cuando la OEI identifique el incumplimiento de la presente directiva remitirá el reporte o denuncia correspondiente a la jefatura correspondiente y de ser el caso al Órgano de Control Interno, para los efectos de su competencia y atribuciones.

DE LA SEGURIDAD DE INFORMACION

Artículo 5°.- Los mecanismos de control y acceso físico para el personal y terceros deben permitir el acceso a las instalaciones y áreas restringidas tecnológicas del HNSEB, SÓLO A PERSONAS AUTORIZADAS para la salvaguarda de los equipos de cómputo y de comunicaciones, así como las instalaciones y los diferentes recursos y sistemas informáticos.

Artículo 6°.- Resguardo y protección de la información y tecnología, es de responsabilidad del usuario reportar de forma inmediata, cuando detecte que existan riesgos reales o potenciales para equipos de cómputo o comunicaciones, como pueden ser fugas de agua, incendio u otros.

Artículo 7°.- El usuario y/o jefatura tiene la obligación de proteger los CD-ROM, DVDs, memorias USB, tarjetas de memoria, discos externos, computadoras y dispositivos portátiles que se encuentren bajo su administración, aun cuando no se utilicen y contengan información reservada o confidencial.

Artículo 8°.- Los usuario deberá informar al superior o responsable de su ámbito sobre aspectos relevantes que afecten la operatividad y/o seguridad del bien o servicio.

Artículo 9°.- Es responsabilidad del usuario evitar en todo momento la fuga de la información del Hospital Sergio E. Bernales que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.

Artículo 10°.- Es de responsabilidad de cada Unidad, departamento, área y/o servicio, los recursos y Equipos informáticos que se le asignen contemplando que su acceso a cualquier usuario ajeno es restringido, por lo que sólo el personal autorizado por la Jefatura y/o personal técnico puede acceder a ellos.

DE LA SEGURIDAD FISICA

Artículo 11°.- Todo desplazamiento de equipo informático perteneciente a la institución, deberá ser coordinado con personal de control patrimonial, equipo de trabajo de informática, Jefe o director del órgano responsable del mismo.

Artículo 12°.- Los usuarios no deben mover o reubicar los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización de la Jefatura, debiendo solicitar el soporte técnico.

Artículo 13°.-En caso de reubicación, previamente debe solicitar a la OEI la viabilidad para no quedar desabastecido del servicio de red (de ser el caso).

Artículo 14°.- Los directores y/o jefes de cada órgano o unidad orgánica del Hospital serán los responsables de informar sobre el uso permanente y/o compartido de algún bien o servicio informático del Hospital; así como sus relevancias y/o cambios respectivos.

Artículo 15°.- El área de soporte técnico de la OEI será la encargada de generar el resguardo y recabar la firma del usuario del equipo informático como responsable de los activos informáticos que se le asignen y de conservarlos en la ubicación autorizada por la Jefatura.

Artículo 16°.- El equipo de cómputo asignado, deberá ser para uso exclusivo de las funciones asignadas al usuario del HNSEB.

Artículo 17°.- Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.

Artículo 18°.-Mientras se opera el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos, a menos que sea en botellas de plástico y estén correctamente cerradas.

Artículo 19°.- Se debe evitar colocar objetos encima de los equipos informáticos y/o o cubrir los orificios de ventilación.

Artículo 20°.- Se debe mantener los equipos informáticos en un entorno limpio y sin humedad.

Artículo 21°.- El usuario debe asegurarse que los cables de conexión no sean pisados o aplastados al colocar otros objetos encima o contra ellos.

Artículo 22°.- Cuando se requiera realizar cambios múltiples del equipo de cómputo derivado de reubicación de lugares físicos de trabajo, éstos deberán ser notificados con dos días hábiles de anticipación a la OEI por conducto regular a través de una solicitud realizada por el titular del área que corresponda.

Artículo 23°.- Queda prohibido que el usuario abra o desarme los equipos de cómputo, porque con ello perdería la garantía que proporciona el proveedor de dicho equipo

Artículo 24°.- Únicamente el personal autorizado de la OEI podrá llevar a cabo los servicios y reparaciones al equipo informático, por lo que los usuarios deberán solicitar la identificación del personal designado antes de permitir el acceso a sus equipos.

Artículo 25°.- El usuario que tenga bajo su resguardo algún equipo de cómputo será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de

acuerdo a la normatividad vigente en los casos de robo, extravío o pérdida del mismo.

Artículo 26°.- El resguardo para las laptops, tiene el carácter de personal y será intransferible. Por tal motivo, queda prohibido su préstamo salvo por mandato expreso de su jefatura y/o Dirección General.

Artículo 27°.- El usuario deberá dar aviso de inmediato a la OEI de la desaparición, robo o extravío del equipo de cómputo o accesorios bajo su resguardo.

Artículo 28°.- El uso de los grabadores de discos compactos es exclusivo para respaldos de información que por su volumen así lo justifiquen.

Artículo 29°.- El usuario que tenga bajo su resguardo este tipo de dispositivos será responsable del buen uso que se le dé.

Artículo 30°.- Los módems internos deberán y solo podrán conectarse de manera directa a las computadoras portátiles y no se deberán utilizar dentro de las instalaciones de la institución para conectarse a ningún servicio de información externo, excepto cuando lo autorice la OEI.

Artículo 31°.- El equipo de cómputo o cualquier recurso de tecnología de información que sufra alguna descompostura por maltrato, descuido o negligencia comprobada por parte del usuario, deberá cubrir el valor de la reparación o reposición del equipo o accesorio afectado. Para tal caso la determinará la causa de dicha descompostura.

DEL MANEJO DE LA INFORMACION

Artículo 32°.- Es responsabilidad de los usuarios almacenar su información únicamente en el directorio o unidad de trabajo que se le asigne, ya que los otros están destinados para archivos, sistemas, programas y sistema operativo.

Artículo 33°.- Los usuarios deberán asegurarse de respaldar la información que considere relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo previendo así la pérdida involuntaria de información, derivada de proceso de reparación, solicitando la asesoría del personal Técnico de la OEI.

Artículo 34°.- Los usuarios deberán utilizar los mecanismos institucionales para proteger la información que reside y utiliza la infraestructura del . De igual forma, deberán proteger la información reservada o confidencial que por necesidades institucionales deba ser almacenada o transmitida, ya sea dentro de la red interna (Dominio) o hacia redes externas como internet.

Artículo 35°.- Los usuarios deberán respaldar de manera periódica la información sensible y crítica que se encuentre en sus computadoras personales o estaciones de trabajo, solicitando asesoría de la OEI para que dichos técnicos determinen el medio y el proceso en que se realizará dicho respaldo.

Artículo 36°.- En caso de que por el volumen de información se requiera algún respaldo en CD, este servicio deberá solicitarse por escrito a la OEI, y deberá contar con la firma del Jefe del área solicitante y adjuntar su medio de almacenamiento a guardar.

Artículo 37°.- Los usuarios del HSEB que hagan uso de equipo de cómputo, deben conocer y aplicar las medidas para la prevención de código malicioso como pueden ser virus, malware o spyware. El usuario puede acudir a la OEI, para solicitar asesoría.

Artículo 38°.- Toda solicitud para utilizar un medio de almacenamiento de información compartido, deberá contar con la autorización del jefe o responsable inmediato del usuario y del titular del área dueña de la información. Dicha solicitud deberá explicar en forma clara y concisa los fines para los que se otorgará la autorización, ese documento se presentará con sello y firma del titular de área la cual se presentara a la OEI para su autorización.

Artículo 39°.- Las actividades que realicen los usuarios del HNSEB en la infraestructura de Tecnología de la Información son registradas y susceptibles de auditoría.

Artículo 40°.- Cuando exista la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización de las unidades administrativas competentes, el usuario informático deberá notificar a su jefe inmediato.

Artículo 41°.- Está prohibido el uso de unidades extraíbles y/o USB en los equipos informáticos del HSEB salvo con autorización de su jefatura, para lo cual se restringirá el acceso de los USB de los equipos.

Artículo 42.- Las jefaturas de las oficinas y/o servicios que deseen crear carpetas compartidas deben informar a la OEI para su respectiva configuración e indicar que personas y maquinas tendrá acceso y tipo de privilegio por usuario (lectura, modificar, eliminar). Si es de terminante prohibido. (Anexo 3)

Articulo 43.- Está prohibido copiar, grabar, eliminar y/o modificar cualquier tipo de archivo dentro de los servidores institucionales que albergan los sistemas hospitalarios y/o administrativos.

Artículo 44°.- Están prohibidas las conexiones de unidades de red que no son designadas por la OEI.

SOBRE SOFTWARE ADICIONAL

Artículo 45°.- Los usuarios que requieran la instalación de software adicional deberán justificar su uso y solicitar formalmente la autorización de la OEI, a través de un memorándum firmado por el Jefe del área para que sea considerado en el Plan Anual de Adquisiciones y adjuntar el Anexo 5.

Artículo 46°.- Se considera una falta grave el que los usuarios instalen cualquier tipo de programa (software) en sus computadoras, estaciones de trabajo, servidores, o cualquier equipo conectado a la red del HNSEB, que no esté autorizado por la OEI.

Artículo 47°.- Está prohibido la instalación de programas para los cuales no exista licencia (productos piratas) o no hayan sido adquiridos por el hospital; por lo que los usuarios se abstendrán de solicitarlos.

SOBRE SOFTWARE ACCESO REMOTO

Artículo 48°.- Esta terminante prohibida la utilización de acceso remoto interno para usuarios no autorizados por la oficina de OEI.

Artículo 49°.- Esta terminante prohibido la utilización e instalación de software de acceso remoto externo, solo puede ser solicitado bajo responsabilidad de la jefatura quien notificara de carácter formal indicando el objetivo y la justificación adjuntando a la misma un documento en calidad de compromiso de asumir la responsabilidad del funcionamiento y/o uso, en el cual detallara el nombre del equipo informático y el usuario que tendrá acceso.

SEGURIDAD DE LA RED

Artículo 50°.- Los usuarios de las áreas del HNSEB no deben establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo de transferencia de archivos (FTP), u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red del HNSEB, sin la autorización por escrito de la OEI.

Artículo 51°.- Será considerado como un ataque a la seguridad informática y una falta grave, cualquier actividad no autorizada por la OEI en la cual los usuarios realicen la exploración de los recursos informáticos en la red del HNSEB, así como

de las aplicaciones que sobre dicha red operan, con fines de detectar y mostrar una posible vulnerabilidad.

Artículo 52°.- Los usuarios no pueden hacer cambio en la configuración de sus redes físicas y/o conexiones (Ip, proxy si fuera el caso etc.).

Artículo 53°.- No está autorizada la instalación de puntos de acceso inalámbricos (Access Point-wifi) que se encuentren fuera de la administración (configuración y supervisión) de la oficina de estadística e informática, porque implican una brecha de seguridad a la información que se maneja dentro de la institución.

Artículo 54°.- Está prohibido el acceso a redes externas por vía de cualquier dispositivo, cualquier excepción deberá ser documentada y contar con el visto bueno de la OEI.

DEL USO DEL CORREO INSTITUCIONAL

Artículo 55°.- Los usuarios no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros. Si fuera necesario leer el correo de alguien más (mientras esta persona se encuentra fuera o ausente), el usuario ausente debe redireccionar el correo a otra cuenta de correo interno, quedando prohibido hacerlo a una dirección de correo electrónico externa al HNSEB, a menos que cuente con la autorización del Jefe del área.

Artículo 56°.- Los usuarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información que es propiedad del HNSEB. Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.

Artículo 57°.- Los usuarios podrán enviar información reservada y/o confidencial exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y atribuciones, a través del correo institucional que le proporcionó la OEI.

Artículo 58°.- El usuario debe de utilizar el correo electrónico institucional del HNSEB, única y exclusivamente para los recursos que tenga asignados y las facultades que les hayan sido atribuidas para el desempeño de su empleo, cargo o comisión, quedando prohibido cualquier otro uso distinto.

Artículo 59°.- Queda prohibido falsear, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.

DE LA SEGURIDAD CONTRA CODIGOS MALICIOSOS Y/O VIRUS

Artículo 60°.- Para prevenir infecciones por virus informáticos, los usuarios del HNSEB, deben evitar hacer uso de cualquier clase de software que no haya sido proporcionado y validado por la OEI.

Artículo 61°.- Los usuarios del HNSEB, deben verificar que la información y los medios de almacenamiento, considerando al menos memorias USB, discos flexibles, CD´s, estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software antivirus autorizado por la OEI.

Artículo 62°.- El usuario debe verificar mediante el software de antivirus autorizado por la Dirección que estén libres de virus todos los archivos de computadora, bases de datos, documentos u hojas de cálculo, etc. que sean proporcionados por personal externo o interno, considerando que tengan que ser descomprimidos.

Artículo 63°.- Ningún usuario del HNSEB debe intencionalmente escribir, generar, compilar, copiar, propagar, ejecutar o tratar de introducir código (programa) conocidos como virus, malware, spyware, o similares de computadora diseñado para autoreplicarse, dañar o en otros casos impedir el funcionamiento de cualquier memoria de computadora, archivos de sistema o software. Tampoco debe probarlos en cualquiera de los ambientes o plataformas del HNSEB. El incumplimiento de este estándar será considerado una falta grave.

Artículo 64°.- Ningún usuario ni empleado de la OEI o personal externo podrá bajar o descargar software de sistemas, sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización de la OEI.

Artículo 65°.- Cualquier usuario que sospeche de alguna infección por virus de computadora, deberá dejar de usar inmediatamente el equipo y llamar a la OEI para la detección y erradicación del virus.

Artículo 66°.- Cada usuario que tenga bajo su resguardo algún equipo de cómputo personal portátil, será responsable de solicitar de manera periódica a la OEI las actualizaciones del software de antivirus.

Artículo 67°.- Los usuarios no deberán alterar o eliminar las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas por la Dirección en programas tales como:

- ✓ Antivirus;
- ✓ Correo electrónico;
- ✓ Paquetería Office;
- ✓ Navegadores; u
- ✓ Otros programas.

Artículo 68°.- Debido a que algunos virus son extremadamente complejos, ningún usuario del HNSEB debe intentar erradicarlos de las computadoras, lo indicado es llamar al personal de la OEI para que sean ellos quienes lo solucionen.

SOBRE EL ACCESO A INTERNET

Artículo 69°.- El acceso a internet provisto a los usuarios del HNSEB es exclusivamente para las actividades relacionadas con las necesidades del puesto y función que desempeña. En caso de daño a la imagen de la institución se procederá de acuerdo a lo que determine el Órgano Interno de Control del HNSEB.

Artículo 70°.- La asignación del servicio de internet, deberá solicitarse por escrito a la OEI, señalando los motivos por los que se desea el servicio. Esta solicitud deberá contar con el visto bueno del Jefe del área correspondiente. (Anexo 4)

Artículo 71°.- Todos los accesos a internet tienen que ser realizados a través de los canales de acceso provistos por HNSEB.

Artículo 72°.- Los usuarios con acceso a Internet del HNSEB tienen que reportar todos los incidentes de seguridad informática inmediatamente después de su identificación, indicando claramente que se trata de un incidente de seguridad informática.

Artículo 73°.- El acceso y uso de los módem del HNSEB tienen que ser previamente autorizado por la OEI.

Artículo 74°.- Los usuarios con servicio de navegación en internet al utilizar el servicio aceptan que:

- ✓ Serán sujetos de monitoreo de las actividades que realizan en internet.
- ✓ Saben que existe la prohibición al acceso de páginas no autorizadas.
- ✓ Saben que existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados.
- ✓ Saben que existe la prohibición de descarga de software sin la autorización de la OEI.
- ✓ La utilización de internet es para el DESEMPEÑO DE SU FUNCIÓN y puesto en el HNSEB y NO PARA PROPÓSITOS PERSONALES.

Artículo 75°.- No está permitido degradar el ancho de banda de la conexión del internet, debido a descargar de archivos de música, imágenes, videos o empleo de radio o video en línea no autorizado.

Artículo 76°.- Los esquemas de permisos de acceso a internet:

NIVEL 1: Sin restricciones: Los usuarios podrán navegar en las páginas que así deseen, así como realizar descargas de información multimedia en sus diferentes presentaciones y acceso total a servicios de mensajería instantánea.

NIVEL 2: Internet restringido, información multimedia y mensajería instantánea: Los usuarios podrán hacer uso de internet (Paginas estatales y otras de conocimiento), páginas de contenido multimedia y red.

NIVEL 3: Internet restringido: Los usuarios podrán hacer uso solo de internet (Paginas estatales y otras de conocimiento) y red.

NIVEL 4: El usuario no tendrá acceso a Internet pero si a la red.

Páginas de contenido para adulto son restringidas completamente en todos los casos.

Se pobra agregara otros nivel de acuerdo al crecimiento y necesidad de la organización.

DE LOS CONTROLES DE ACCESO LÓGICO

Artículo 77°.- Cada usuario es responsable del mecanismo de control de acceso que le sea proporcionado; su identificador de usuario (userID) y contraseña (password) necesarios para acceder a la información y a la infraestructura tecnológica del HNSEB, por lo cual deberá mantenerlo de forma confidencial.

Artículo 78°.- Las Jefaturas de cada área serán las responsables de remitir la información pertinente a creación de usuarios nuevos (identificadores de PC), como de usuarios que ya no pertenecen a su área o institución para restringir y/o reubicar su acceso (actualización). (Anexo 1)

Artículo 79°.- El Jefe de la OEI o el responsable, es el único que puede otorgar la autorización para que se tenga acceso a la información que se encuentra en la infraestructura tecnológica del HNSEB, otorgándose los permisos mínimos necesarios para el desempeño de sus funciones, con apego al principio "Necesidad de saber".

Artículo 80°.- El acceso a la infraestructura tecnológica y/o sistemas del HNSEB para personal externo debe ser autorizado por el jefe de la oficina y/o Área, quien deberá notificarlo formalmente a la OEI, quien lo habilitará. (Anexo 2)

Artículo 81°.- Está prohibido que los usuarios utilicen la infraestructura tecnológica del HNSEB para obtener acceso no autorizado a la información u otros sistemas de información.

Artículo 82°.- Cualquier cambio en los roles y responsabilidades de los usuarios que modifique sus privilegios de acceso a la infraestructura tecnológica del HNSEB, deberán ser notificados por escrito o vía correo electrónico a la OEI con el visto bueno del titular del área solicitante, para realizar el ajuste.

RESPONSABILIDAD DE LOS USUARIOS

Artículo 83°.- Todos los usuarios de servicios de información son responsables por su identificador de usuario y contraseña que recibe para el uso y acceso de los recursos.

Artículo 84°.- Todos los usuarios deberán autenticarse por los mecanismos de control de acceso provistos por la OEI antes de poder usar la infraestructura tecnológica del HNSEB.

Artículo 85°.- Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica del HNSEB, a menos que se tenga autorización de la OEI.

Artículo 86°.- Cada usuario que accede a la infraestructura tecnológica del HNSEB debe contar con un identificador de usuario único y personalizado, por lo cual no está permitido el uso de un mismo identificador de usuario por varios usuarios excepto en áreas de rotación constante por turnos.

Artículo 87°.- Los usuarios tienen prohibido compartir su identificador de usuario y contraseña (Identificador Pc y usuario de Sistemas), ya que todo lo que ocurra con ese identificador y contraseña será responsabilidad exclusiva del usuario al que pertenezcan, salvo prueba de que le fueron usurpados esos controles.

Artículo 88°.- Los usuarios tienen prohibido usar el identificador y/o usuario y contraseña de otros, aunque ellos les insistan en usarlo.

Artículo 89°.- Los usuarios deberán mantener sus equipos de cómputo con controles de acceso como contraseñas y bloqueo, como una medida de seguridad cuando el usuario necesita ausentarse de su escritorio por un tiempo.

Artículo 90°.- Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá reportarlo A la OEI por correo electrónico, indicando si es de acceso a la red o a módulos de sistemas desarrollados por la Dirección, para que se le proporcione una nueva contraseña.

Artículo 91°.- La obtención o cambio de una contraseña debe hacerse de forma segura; el usuario deberá acreditarse ante la OEI como empleado del HNSEB.

Artículo 92°.- Está prohibido que los identificadores de usuarios y contraseñas se encuentren de forma visible en cualquier medio impreso o escrito en el área de trabajo del usuario, de manera de que se permita a personas no autorizadas su conocimiento.

Artículo 93°.- Todos los usuarios deberán observar los siguientes lineamientos para la construcción de sus contraseñas:

- No deben contener números consecutivos;
- Deben estar compuestos de al menos seis (6) caracteres y máximo diez (10). Estos caracteres deben ser alfanuméricos, o sea, números y letras;
- Deben ser difíciles de adivinar, esto implica que las contraseñas no deben relacionarse con el trabajo o la vida personal del usuario; y
- Deben ser diferentes a las contraseñas que se hayan usado previamente.

Artículo 94°.- La contraseña podrá ser cambiada por requerimiento del dueño de la cuenta.

Artículo 95°.- Todo usuario que tenga la sospecha de que su contraseña es conocida por otra persona, tendrá la obligación de cambiarlo inmediatamente.

Artículo 96°.- Los usuarios no deben almacenar las contraseñas en ningún programa o sistema que proporcione esta facilidad.

Artículo 97°.- Los cambios o desbloqueo de contraseñas solicitados por el usuario a la OEI serán solicitados formalmente y firmado por el jefe inmediato del usuario que lo requiere.

DE LAS ACCCIONES DE LA OEI

Artículo 98°.- La Oficina de Estadística e Informática, es la encargada de fijar las bases de la política informática que permitan conocer y planear el desarrollo tecnológico del HNSEB.

Artículo 99°.- La OEI realizará acciones de verificación del cumplimiento del de las Políticas y Estándares de Seguridad Informática para usuarios.

Artículo 100°.- La OEI podrá implementar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo, para revisar la actividad de procesos que ejecuta y la estructura de los archivos que se procesan. El mal uso de los recursos informáticos que sea detectado será reportado conforme a lo indicado en la Política de Seguridad.

Artículo 101°.- Asistir al usuario que sospeche o tenga conocimiento de la ocurrencia de un incidente de seguridad informática.

Artículo 102°.- Reportar a la jefatura correspondiente si se vulnera o encuentra indicios de falta a la presente directiva.

DE LOS DERECHOS DE PROPIEDAD INTELECTUAL

Artículo 103°.- Está prohibido por las leyes de derechos de autor y por el HNSEB, realizar copia no autorizadas de software, ya sea adquirido o desarrollado por el HNSEB.

Artículo 104°.- Los sistemas desarrollados por personal, interno o externo, que sea parte de la OEI, o sea coordinado por ésta, son propiedad intelectual del HNSEB.

VII. RESPONSABILIDADES

La presente directiva será distribuida a los jefes de las Unidades Orgánicas que conforman el Hospital, bajo responsabilidad funcional y quienes deben dar y hacer cumplir la presente directiva.

La Oficina de Estadística e informática es responsable de la supervisión y difusión del presente documento.

El periodo de revisión de la presente directiva es anual, donde intervendrán la Oficina de Estadística e Informática en la formulación y elaboración, y la Oficina de Planeamiento Estratégico para la opinión técnica.

VIII. DISPOSICIONES COMPLEMENTARIAS Y FINALES

La presente Directiva Administrativa, entrara en vigencia a partir del día siguiente de su aprobación.

IX. ANEXOS:

ANEXO 1: MODELO DE SOLICITUD DE CREACION, MOVIMIENTO O BAJA, DEL IDENTIFICADOR DE USUARIO Y/O MODIFICACION DE CONTRASEÑA.

ANEXO 2: MODELO DE SOLICITUD DE CREACION O BAJA DE USUARIO SISTEMAS HOSPITALARIOS

ANEXO 3: MODELO DE SOLICITUD DE ATENCIONES

ANEXO 4: MODELO DE SOLICITUD DE ACCESO DE INTERNET

AENXO 5: MODELO DE SOLICITUD DE INSTALACION DE SOFTWARE ADICIONAL

PERU | Ministerio de Salud | Instituto de Gestión de Servicios de Salud | Hospital Nacional Sergio E. Bernales

ANEXO 1

FORMATO DE SOLICITUD DE IDENTIFICADOR DE USUARIO PARA ACCESO A EQUIPOS INFORMÁTICOS DE HNSEB

Oficina o Servicio: _____ Sub Area: _____

Fecha: ___/___/_____

Tipo de Tramite:

1. CREACION: ☐ 3. BAJA: ☐ 5. OTROS:
2. MODIFICACION: ☐ 4. CAMBIO DE CLAVE: ☐

Nombres y Apellidos (usuario): _____ Nombre de PC designada: _____

2	Dpto. y Area anterior de Trabajo : _____ Nuevo Dpto. y Area de Trabajo :
3	Temporal: ☐ Motivo: _____ Definitiva: ☐
5	Descripción del tramite respecto al identificador de Usuario de PC a Solicitar:

Jefe(a) Dpto. o Oficina Solicitante
Firma y sello

Usuario
Firma y Huella*

ANEXO 2

PERU | Ministerio de Salud | Instituto de Gestión de Servicios de Salud | Hospital Nacional Sergio E. Bernales

FORMATO DE SOLICITUD DE ACCESO A SISTEMAS INFORMÁTICOS DE HNSEB

Oficina o Servicio: _____ Sub Area: _____

Nombres y Apellidos (usuario): _____ Nombre de PC designada: _____

Sistema: _____ Fecha: ___/___/_____

Tipo de Tramite:

1. INSTALACION: ☐ 3. BAJA: ☐ 5. OTROS: ☐
2. CREACIÓN DE USUARIOS: ☐ 4. CAMBIO DE CLAVE: ☐

3	Temporal: ☐ Motivo: _____ Definitiva: ☐
5	Descripción de acceso a otro:

Jefe(a) Dpto. o Oficina Solicitante
Firma y sello

Usuario
Firma y Huella*

PERU | Ministerio de Salud | Instit de Gestión de Servicios de Salud | Hospital Nacional Sergio E. Bernales

ANEXO 3

FORMATO DE SOLICITUD DE ATENCIONES DE SERVICIOS INFORMÁTICOS DE HNSEB

Oficina o Servicio: _____ **Sub Area:** _____

Fecha: ___/___/_____

Tipo de Tramite:

1. CREACIÓN CARPETAS COMPARTIDAS ☐ 2. INSTALACIÓN DE IMPRESORAS ☐ 3. OTROS: _____

N°	NOMBRE DE USUARIO	USUARIO	N° PC	PRIVILEGIO
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				
26				
27				

MINISTERIO DE SALUD – HOSPITAL SERGIO E. BERNALES – Estadística e Informática

HOSP. SERGIO E. BERNALES – ORGANIZACIÓN

Jefe(a) Dpto. o Oficina Solicitante
Firma y sello

firma de usuarios:

1 _____ 4 _____ 7 _____ 14 _____ 21 _____

2 _____ 5 _____ 8 _____ 15 _____ 22 _____

3 _____ 6 _____ 9 _____ 16 _____ 23 _____

10 _____ 17 _____ 24 _____

11 _____ 18 _____ 25 _____

12 _____ 19 _____ 26 _____

13 _____ 20 _____ 27 _____

PERU | Ministerio de Salud | Instit de Gestión de Servicios de Salud | Hospital Nacional Sergio E. Bernales

ANEXO 4

FORMATO DE SOLICITUD DE ACCESO DE INTERNET

Oficina o Servicio: _____ Sub Area: _____

Fecha: ___/____/_____

Tipo de Servicio:

1. ACCESO NUEVO ☐ 2. MODIFICACIÓN DE NIVEL ☐ 3. OTROS: ☐

N°	USUARIO RESPONSABLE (NOMBRE COMPLETO)	IDENTIFICADOR DE USUARIO	NOMBRE EQUIPO	NIVEL DE ACCESO

Observaciones:

3

Jefe(a) Dpto. o Oficina Solicitante
Firma y sello

MINISTERIO DE SALUD – HOSPITAL SERGIO BERNALES – Estadística e Informática

HOSP. SERGIO E. BERNALES – ORGANIZACIÓN

MINISTERIO DE SALUD – DIRECCIÓN GENERAL – Hospital Nacional Sergio E. Bernales

PERU | Ministerio de Salud | Instituto de Gestión de Servicios de Salud | Hospital Nacional Sergio E. Bernales

ANEXO 5

FORMATO DE SOLICITUD DE SOFTWARE ADICIONAL DENTRO DEL HNSEB

Fecha: ___/___/_____

Oficina o Servicio: _____ Sub Area:

Software Requerido: _____ Tiempo de Uso: _____

	Nombres y Apellidos (usuario):	Identificador	Nombre de PC

Justificación del requerimiento:

Jefe(a) Dpto. o Oficina Solicitante
Firma y sello

Usuario
Firma y Huella*

MINISTERIO DE SALUD HOSPITAL SERGIO E. BERNALES Of. Estadística e Informática

HOSP. SERGIO E. BERNALES ORGANIZACION

MINISTERIO DE SALUD DIRECCION GENERAL Hospital Nacional Sergio E. Bernales